

**Permissions Overview**

**Purpose:** This document outlines the permissions and access controls assigned to different roles across various environments (Development, Test, and Production) for database and reporting systems. The permissions are categorized for developers, quality assurance (QA) users, data analysts, ETL (Extract, Transform, Load) teams, and users working with SQL Server Reporting Services (SSRS) and SQL Server Analysis Services (SSAS). It defines the specific levels of access to ensure the security and integrity of the database environments while allowing each role to perform its required tasks efficiently.

The purpose of this document is to:

* Clarify the roles and responsibilities for database and reporting operations.
* Ensure proper access control management based on the environment and the function of each team.
* Promote secure and appropriate data access for development, testing, and production activities.

**Developer Permissions**

Developers have varying levels of access depending on the environment. The DBO schema primarily provides database-level permissions. Below are the access levels for each environment:

DEV: Full rights (db\_owner)  
Developers can perform all actions, including creating, altering, and dropping database objects (e.g., tables, and stored procedures) in the development environment.

TST: Read/Write/Execute/View Definitions  
Developers have permission to read, modify data, execute stored procedures, and view the definitions of database objects in the test environment.

STG/PRD: Read/View Definitions  
In the production environment, developers can only read data and view the definitions of database objects without modifying them.

**Read-Only Permissions (QA)**

Quality Assurance (QA) users have restricted permissions across environments. They are primarily responsible for running queries and reports without making changes to the data:

DEV/TST/STG/PRD: Read-Only for all tables  
QA users can read data in all tables but cannot modify or execute data operations in any environment.

Run SSRS reports  
QA users can access and run SQL Server Reporting Services (SSRS) reports across all environments.

**SSAS Permissions (Data Analysts)**

Data Analysts typically work with SQL Server Analysis Services (SSAS) and require permissions to analyze data across environments:

NONPRD: Execute Stored Procedures  
Data analysts can run stored procedures in non-production environments.

DEV: Write to all tables  
In the development environment, data analysts have permission to modify and write data to tables.

DEV/TST/STG/PRD: Read all tables/View Definitions  
Data analysts can view and read data from all tables and view database object definitions across development, test, and production environments.

**SSIS Permissions (ETL): SSIS Schema**

ETL (Extract, Transform, Load) teams working with SQL Server Integration Services (SSIS) have specific permissions related to data processing and job management in the SSIS schema:

NONPRD: Execute Stored Procedures  
ETL users can execute stored procedures in non-production environments.

DEV/TST/PRD: Read-Only for all tables  
In all environments, ETL users can read data but are not allowed to write or modify it.

DEV/TST/PRD: Start Agent Jobs  
ETL users can start and manage SQL Server Agent Jobs in all environments to handle scheduled tasks like data transfers and transformations.

**SSRS Permissions**

Permissions for publishing and accessing SQL Server Reporting Services (SSRS) reports vary depending on the environment:

DEV: Publish SSRS reports  
In the development environment, users can create and publish new SSRS reports.

DEV/TST/PRD: Read-Only for all tables  
SSRS users can read data from all tables without modifying or deleting it across development, test, and production environments.

**IT System Administrators Permissions**

System administrators have standardized permissions across all environments. They own all application databases (excluding SYSTEM, DBA, and Perfstats databases) and can perform any necessary functions. Additionally, they have server-level access to view server states.

Reference other documentation:

[PermissionsGivenByDefault.docx](https://alliedsolutions.sharepoint.com/:w:/r/teams/DatabaseServices/Shared%20Documents/Documentation/Standards/PermissionsGivenByDefault.docx?d=wd21ad7d06c58487f98ff9721f3c346a8&csf=1&web=1&e=pfC4tN)

[SQL Server Access Request Standards.docx](https://alliedsolutions.sharepoint.com/:w:/r/teams/DatabaseServices/Shared%20Documents/Documentation/Standards/SQL%20Server%20Access%20Request%20Standards.docx?d=w0151a984c5ca4edc8d5089dd7e0b03d3&csf=1&web=1&e=lj8brS)